Amendments To The Claims

The following listing of claims replaces all prior versions and listings of claims in the application.

Listing of Claims

1. (Currently Amended) A master digital data creation device for supplying second digital data obtained by scrambling first digital data to a digital data reproduction device having a recording medium, comprising:

an encryption block generating a first control word for identifying ~~based on~~ an allowable number of reproductions specified by the digital data reproduction device and applying a one-way function to the first control word a number of times corresponding to the allowable number of reproductions to generate a second control word for scrambling the first digital data and representing a number of times said first digital data has been reproduced;

a scrambler receiving the second control word ~~for scrambling the first digital data~~ and using the second control word to produce the second digital data; and

an output block outputting the second digital data and the first control word to the digital data reproduction device.

2. (Currently Amended) A digital data reproduction device comprising:

an acceptor accepting recording media on which first digital data and a first control word [[CW_k]] are recorded, said first control word being generated based on a specified allowable number k of reproductions and being an identifier of said allowable number k of reproductions, said first digital data [[being]] having been generated by scrambling desired

second digital data using a second control word [[CW_o]] having been generated by applying a one-way function to the first control word [[CW_k]] k times;

a decryption block receiving the first control word [[CW_k]] and applying the one-way function to the first control word [[CW_k]] k times to produce the second control word [[CW_0]];

a de-scrambler receiving the first digital data and the second control word [[CW_o]] and de-scrambling the first digital data using the second control word [[CW_o]] to produce the second digital data; and

a reproduction unit reproducing the second digital data generated by said de-scrambler,

wherein, after every reproduction by said reproduction unit, said decryption block writes a third control word ~~$CW_{(k-1)}$~~ back to said recording media representing a remaining number of allowable reproductions of said second digital data, said third control word ~~$CW_{(k-1)}$~~ being generated by applying the one-way function to the first control word [[CW_k]] once, and wherein, if the first control word [[CW_K]] received from the recording media equals the second control word [[CW_0]], the de-scrambling by said de-scrambler and the reproduction by said reproduction unit are inhibited.

3. (Currently Amended) The digital data reproduction device according to claim 2, wherein, when a desired number of reproductions, n, is received from some other reproduction device, said decryption block receives the first control word [[CW_k]] from the recording media and, if $k \geq n$, applies the one-way function to the first control word [[CW_k]] (k-n) times to produce the third control word [[CW_n]] representing a remaining number of

allowable reproductions of said second digital data and applies the one-way function to the first control word [[CW_k]] n times to produce the fourth control word ~~$CW_{(k-n)}$~~ representing a replacement identifier for said first control world for representing an allowable number of reproductions of said second digital data; and records the fourth control word ~~$CW_{(k-n)}$~~ on the recording media for updating, further comprising:

an output block outputting the first digital data recorded on the recording media, and the third control word [[CW_n]], obtained from the decryption block, to the other reproduction device.